学号：U201814779　　班级：CS1806　　姓名：黄宗煜

一、必答题

PA1

1. **我选择的ISA是** *riscv32*
2. **理解基础设施**

   $500 * 90\% * 30 * 20 = 270000s = 75h$

   一学期将要花费 75 个小时的时间在调试上。

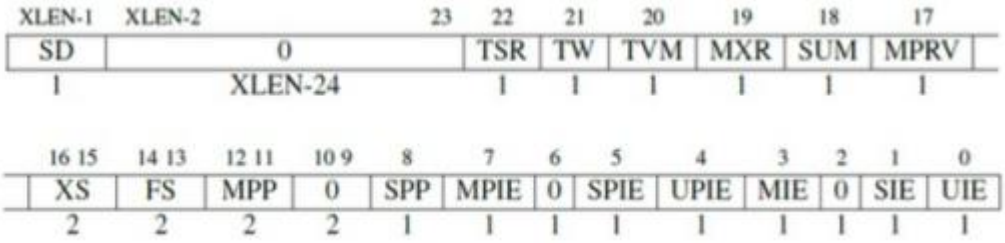
   $500 * 90\% * 20 * 20 = 180000s = 50h$

   一学期可以节省 50 个小时调试的时间。
3. **查阅 riscv32 手册**
   - **riscv32有哪几种指令格式?**

     6种
   - **LUI指令的行为是什么?**

     `LUI`指令的行为是高位立即数加载
   - **mstatus寄存器的结构是怎么样的?**

     根据文档可知`mstatus`寄存器的结构如下所示



4. **完成PA1的内容之后, `nemu/` 目录下的所有.c和.h和文件总共有多少行代码? 你是使用什么命令得到这个结果的? 和框架代码相比, 你在PA1中编写了多少行代码? (Hint: 目前 `pa1` 分支中记录的正好是做PA1之前的状态, 思考一下应该如何回到"过去"?) 你可以把这条命令写入 `Makefile` 中, 随着实验进度的推进, 你可以很方便地统计工程的代码行数, 例如敲入 `make count` 就会自动运行统计代码行数的命令. 再来个难一点的, 除去空行之外, `nemu/` 目录下的所有 `.c` 和 `.h` 文件总共有多少行代码?**

   通过`git checkout pa1`回到刚完成pa1的状态

   在`nemu/`目录下输入

   ```
   find nemu -name "*.[hc]" | xargs wc -l
   ```

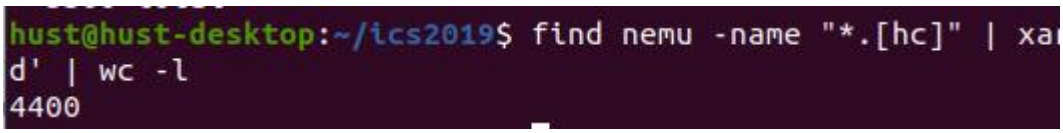
   即可输出`nemu`目录下所有`.c`文件以及`.h`文件的行数，如下图所示

   对于空行可以通过以下指令来去除

   ```
   find nemu -name "*.[hc]" | xargs cat | sed '/^\s*$/d' | wc -l
   ```

   运行结果如下

   利用同样的方法也可以去除所有的空行以及注释，在此不再赘述

5. **打开工程目录下的`Makefile`文件, 你会在`CFLAGS`变量中看到gcc的一些编译选项. 请解释gcc中的`-Wall`和`-Werror`有什么作用? 为什么要使用`-Wall`和`-Werror`?**

   `-Wall` 打开gcc所有的警告

   `-Werror` 将所有的警告当成错误进行处理

   使用`-Wall`以及`-Werror`有利于发现代码中不严谨之处，如类型的隐式转换

PA2

1. **请整理一条指令在NEMU中的执行过程. (我们其实已经在PA2.1阶段提到过这道题了)**

   以`lw`指令为例

   ```
   `isa_exec`函数被执行
     |
     |==>  通过`instr_fetch`函数获得当前`pc`值对应的内存位置中的指令
          调用`idex`，也即`译码-执行`函数
         |
         |==> 调用`decode_ld`函数，获得操作数，将其保存在全局变量`id_src`以及
   `id_dest`中
              调用`exec_load`函数，
             |
             |==>  根据`funct3`字段，索引`load_table`，找到对应的执行函数`exec_ld`，
   同时设定位宽width
                   调用函数`exec_ld`
                   |
                   |==>根据`lw`指令的逻辑，调用rtl函数
                        调用`rtl_lm`将id_src.addr所指向的地址取出decinfo.width宽度的
   数据，保存在临时寄存器s0中
                        调用`rlt_sr`将s0保存在id_dest.reg指向的寄存器中
                        根据宽度调用print_asm_template2打印具体的汇编指令
   ```

2. **在`nemu/include/rtl/rtl.h`中, 你会看到由`static inline`开头定义的各种RTL指令函数. 选择其中一个函数, 分别尝试去掉`static`, 去掉`inline`或去掉两者, 然后重新进行编译, 你可能会看到发生错误. 请分别解释为什么这些错误会发生/不发生? 你有办法证明你的想法吗?**

   - 去掉static 不会发生错误
   - 去掉inline，编译时不会发生错误，链接时会发生错误。LD在链接不同的object时，会发现同一个符号在不同的object中被多次定义，并且我们没有告诉LD这种情况下应该怎么进行链接，因此报错

3. **编译与链接**

   - **在`nemu/include/common.h`中添加一行`volatile static int dummy;`然后重新编译NEMU. 请问重新编译后的NEMU含有多少个`dummy`变量的实体? 你是如何得到这个结果的?**

     一个

   - **添加上题中的代码后, 再在`nemu/include/debug.h`中添加一行`volatile static int dummy;`然后重新编译NEMU. 请问此时的NEMU含有多少个`dummy`变量的实体? 与上题中`dummy`变量实体数目进行比较, 并解释本题的结果.**

     两个

     static关键字表示变量只有在当前文件可以被识别，volatile表示这处代码不会被编译器优化，而`debug.h`通过include包含了`common.h`，所以重新声明的变量不会覆盖之前的dummy

   - **修改添加的代码, 为两处`dummy`变量进行初始化: `volatile static int dummy = 0;`然后重新编译NEMU. 你发现了什么问题? 为什么之前没有出现这样的问题? (回答完本题后可以删除添加的代码.)**

出现重定义

给变量赋值之后，声明就变成了定义，所以会发生重定义问题

4. 请描述你在`nemu/`目录下敲入`make`后, `make`程序如何组织.c和.h文件, 最终生成可执行文件`nemu/build/$ISA-nemu`. (这个问题包括两个方面:`Makefile`的工作方式和编译链接的过程.)

   通过阅读文档中给出的C语言基础中的makefile基础一节以及man文档，可以对makefile有一个基本的了解

   对于Makefile，基本的工作方式如下

   1. 首先依次读取变量“MAKEFILES”定义的 makefile 文件列表
   2. 读取工作目录下的 makefile 文件
   3. 一次读取工作目录下的 makefile 文件指定的 include 文件
   4. 查找重建所有已读的 makefile 文件的规则
   5. 初始化变量值并展开那些需要立即展开的变量和函数并根据预设条件确定执行分支
   6. 建立依赖关系表
   7. 执行 rules

   具体到`/nemu/Makefile`这个文件本身，具体的编译链接过程如下

   1. 首先Makefile默认的ISA为x86，如果定义了具体的ISA，则需要保证其有效
   2. 根据ISA确定需要include的文件列表
   3. 确定编译目标文件夹（默认是`build/`）确定编译器以及链接器（`gcc`）
   4. 设置编译选项`CFLAGS`
   5. 读取所有需要编译的`.c`的文件并将其编译为`.o`文件
   6. 进行链接
   7. 执行`git commit`

PA3

1. **理解上下文结构体的前世今生 (见PA3.1阶段)**

   > 你会在`__am_irq_handle()`中看到有一个上下文结构指针`c`, `c`指向的上下文结构究竟在哪里?这个上下文结构又是怎么来的?具体地,这个上下文结构有很多成员,每一个成员究竟在哪里赋值的?`$ISA-nemu.h`, `trap.S`, 上述讲义文字, 以及你刚刚在NEMU中实现的新指令, 这四部分内容又有什么联系?

`__am_irq_handle`函数在整个项目中，唯一出现的调用文件就是`trap.S`。其中通过`jal`指令直接跳转到对应的函数体，而函数的参数是保存在栈当中的，可以看到在`jal`指令之前有诸多压栈操作，按照顺序是

1. 32个寄存器，通过`MAP(REGS, PUSH)`
2. 成员`cause`，通过`sw t0 OFFSET_CAUSE(sp)`
3. 成员`status`，通过`sw t1 OFFSET_STATUS(sp)`
4. 成员`epc`，通过`sw t2 OFFSET_EPC(sp)`

于是不同的成员被赋值。可以在`_am_irq_handle`函数中被使用

2. 理解穿越时空的旅程 (见PA3.1阶段)

> 从Nanos-lite调用`_yield()`开始, 到从`_yield()`返回的期间, 这一趟旅程具体经历了什么? 软(AM, Nanos-lite)硬(NEMU)件是如何相互协助来完成这趟旅程的? 你需要解释这一过程中的每一处细节, 包括涉及的每一行汇编代码/C代码的行为, 尤其是一些比较关键的指令/变量. 事实上, 上文的必答题"理解上下文结构体的前世今生"已经涵盖了这趟旅程中的一部分, 你可以把它的回答包含进来.

- 首先`_yield`函数，通过内联汇编代码将a7设置为-1，表示当前的ecall类型是`_yield`，接着执行了`ecall`指令。
- 汇编`ecall`指令将会由`ecall`对应的`EHelper`来执行相关的函数，函数中会调用`raise_intr`函数，参数NO即为a7寄存器的值，表示中断号。
- 在`raise_intr`函数中会保存`epc`到`sepc`寄存器，将中断号保存到`scause`寄存器，并从`stvec`获得中断入口地址并进行跳转。也就是`_am_asm_trap`函数的入口地址，也就是汇编代码`trap.S`中的起始位置。开始执行。
- 汇编代码会执行到上述的`_am_irq_handle`函数
- `__am_irq_handle`函数根据`c->cause`来分别进行处理，如果是`-1`就表示yield事件，如果是0到19(支持的系统调用的个数)就说明是系统调用。此处是yield，于是填充ev.event成员为`_EVENT_YIELD`并调用用户定义的回调函数`do_event`
- 同样是根据event的类型来分别处理，如果是`_EVENT_YIELD`就打印出信息到终端，如果是`_EVENT_SYSCALL`的话就调用`do_syscall`，此处是打印信息到终端
- 函数结束之后将会回到`trap.S`汇编代码。恢复上下文并调用`sret`指令
- `sret`指令将会调用nemu中针对`sret`指令的执行函数，从`sepc`寄存器中读出之前保存的pc，将其加4，表示中断发生时的吓一跳指令的地址，并进行跳转

至此`yield`函数执行完毕

3. hello程序是什么, 它从而何来, 要到哪里去 (见PA3.2阶段)

> 我们知道`navy-apps/tests/hello/hello.c`只是一个C源文件, 它会被编译链接成一个ELF文件. 那么, hello程序一开始在哪里? 它是怎么出现内存中的? 为什么会出现在目前的内存位置? 它的第一条指令在哪里? 究竟是怎么执行到它的第一条指令的? hello程序在不断地打印字符串, 每一个字符又是经历了什么才会最终出现在终端上?

- hello程序对应的elf文件会在整个项目编译的时候，将其在ramdisk的偏移位置保存在`files.h`的记录表中(`disk_offset`成员)。
- 接着通过load函数解析对应的elf文件，得到具体的入口地址，保存在`e_entry`中
- 通过`((void(*)())entry) ()`跳转到对应位置进行执行。
- 在main函数中通过printf进行输出，printf函数首先会尝试进行`_brk`，如果失败则一个字符

一个字符的通过`write`输出到终端，如果成功则将字符串作为整体调用`write`进行输出。
    - `write`函数会调用`_write`系统调用，在对应的处理函数中，发现输出的对象是stdout，则直接通过`serial_write`进行输出。
4. **运行仙剑奇侠传时会播放启动动画, 动画中仙鹤在群山中飞过. 这一动画是通过`navy-apps/apps/pal/src/main.c`中的`PAL_SplashScreen()`函数播放的. 阅读这一函数, 可以得知仙鹤的像素信息存放在数据文件`mgo.mkf`中. 请回答以下问题: 库函数, libos, Nanos-lite, AM, NEMU是如何相互协助, 来帮助仙剑奇侠传的代码从`mgo.mkf`文件中读出仙鹤的像素信息, 并且更新到屏幕上? 换一种PA的经典问法: 这个过程究竟经历了些什么?**
    - 在`navy-apps/apps/palc/hal/hal.c`中的 `redraw` 函数中通过 `NDL_DrawRect` 和 `NDL_Render` 更新屏幕。
    - `NDL` 通过之前的初始化操作维护了一块画布`canvas`， 并将其绘制操作限定在该画布上。
    - `NDL_DrawRect` 会将传入的`pixels`保存到会把传入的像素逐个存入画布的对应位置
    - 首先调用了`libndl`库，在该库中会打开设备文件`/dev/fb` 和 `/dev/fbsync`，在接收到该函数调用后会向`/dev/fb` 设备文件中写入，在该函数 中，判断出要写的文件是`/dev/fb` 设备文件之后，会调用 `fb_write` 帮助函数， 之后会调用 `draw_rect` 函数，该函数位于`nexus-ambsibc/io.c` 中，在函数内会调用`_io_write` 函数
    - 而`_io_write`会转发给`_am_video_write` 函数， 该函数中会执行 out 汇编指令，将数据传送给 `vga` 设备中。
    - vga 设备在接收到数 据后会保存在定义的显存中，当之后 NDL 库向`/dev/fbsyn`设备文件中写入时， vga 设备最终会调用 SDL 库来更新画面。
    - `NDL_Render` 函数会对画布的每一行先调用 `fseek` 把偏移量定位到该行起点在屏幕中对应的位置，然后调用 `fwrite` 输出画布的一行，并调用 `fflush()`刷新缓冲，最后调用`putc` 向 `fbsyncdev` 输出 0 进行同步，并调用 `fflush` 刷新缓冲。

二、测试结果以及说明

PA1

不同指令的测试

1. 帮助指令`help`

2. 单步执行`si`

   包含参数缺省值以及指定步数的情况

```
(nemu) si
80100000:    b7 02 00 80                                    lui   0x80000,t0
```

3. 打印寄存器信息`info r`

```
(nemu) info r
$0 = 0x00000000 , ra = 0x00000000 , sp = 0x00000000 , gp = 0x00000000 , tp = 0x00000000 , t0 = 0x80000000 , t1 = 0x00000000 , t2 = 0x00000000
s0 = 0x00000000 , s1 = 0x00000000 , a0 = 0x00000000 , a1 = 0x00000000 , a2 = 0x00000000 , a3 = 0x00000000 , a4 = 0x00000000 , a5 = 0x00000000
a6 = 0x00000000 , a7 = 0x00000000 , s2 = 0x00000000 , s3 = 0x00000000 , s4 = 0x00000000 , s5 = 0x00000000 , s6 = 0x00000000 , s7 = 0x00000000
s8 = 0x00000000 , s9 = 0x00000000 , s10 = 0x00000000 , s11 = 0x00000000 , t3 = 0x00000000 , t4 = 0x00000000 , t5 = 0x00000000 , t6 = 0x0000000
0
pc = 0X80100010
```

4. 表达式求值

```
(nemu) p (1+2)*(4/3)
[src/monitor/debug/expr.c,91,make_token] match rules[7] = "\(" at position 0 with len 1: (
[src/monitor/debug/expr.c,91,make_token] match rules[10] = "[0-9]+" at position 1 with len 1: 1
[src/monitor/debug/expr.c,91,make_token] match rules[1] = "\+" at position 2 with len 1: +
[src/monitor/debug/expr.c,91,make_token] match rules[10] = "[0-9]+" at position 3 with len 1: 2
[src/monitor/debug/expr.c,91,make_token] match rules[8] = "\)" at position 4 with len 1: )
[src/monitor/debug/expr.c,91,make_token] match rules[5] = "\*" at position 5 with len 1: *
[src/monitor/debug/expr.c,91,make_token] match rules[7] = "\(" at position 6 with len 1: (
[src/monitor/debug/expr.c,91,make_token] match rules[10] = "[0-9]+" at position 7 with len 1: 4
[src/monitor/debug/expr.c,91,make_token] match rules[6] = "/" at position 8 with len 1: /
[src/monitor/debug/expr.c,91,make_token] match rules[10] = "[0-9]+" at position 9 with len 1: 3
[src/monitor/debug/expr.c,91,make_token] match rules[8] = "\)" at position 10 with len 1: )
val1:4 / val2:3
 (1+2)*(4/3) = 3(0x3) ;
(nemu) p(3*4)*(3+4
Unknown command 'p(3*4)*(3+4'
(nemu) p (3*4)*(3+4
[src/monitor/debug/expr.c,91,make_token] match rules[7] = "\(" at position 0 with len 1: (
[src/monitor/debug/expr.c,91,make_token] match rules[10] = "[0-9]+" at position 1 with len 1: 3
[src/monitor/debug/expr.c,91,make_token] match rules[5] = "\*" at position 2 with len 1: *
[src/monitor/debug/expr.c,91,make_token] match rules[10] = "[0-9]+" at position 3 with len 1: 4
[src/monitor/debug/expr.c,91,make_token] match rules[8] = "\)" at position 4 with len 1: )
[src/monitor/debug/expr.c,91,make_token] match rules[5] = "\*" at position 5 with len 1: *
[src/monitor/debug/expr.c,91,make_token] match rules[7] = "\(" at position 6 with len 1: (
[src/monitor/debug/expr.c,91,make_token] match rules[10] = "[0-9]+" at position 7 with len 1: 3
[src/monitor/debug/expr.c,91,make_token] match rules[1] = "\+" at position 8 with len 1: +
[src/monitor/debug/expr.c,91,make_token] match rules[10] = "[0-9]+" at position 9 with len 1: 4
Bad expression ! check_parenthese, [0, 9]
```

```
(nemu) p ((10*10)-20+($tp*10)*($s0*5))
[src/monitor/debug/expr.c,91,make_token] match rules[7] = "\(" at position 0 with len 1: (
[src/monitor/debug/expr.c,91,make_token] match rules[7] = "\(" at position 1 with len 1: (
[src/monitor/debug/expr.c,91,make_token] match rules[10] = "[0-9]+" at position 2 with len 2: 10
[src/monitor/debug/expr.c,91,make_token] match rules[5] = "\*" at position 4 with len 1: *
[src/monitor/debug/expr.c,91,make_token] match rules[10] = "[0-9]+" at position 5 with len 2: 10
[src/monitor/debug/expr.c,91,make_token] match rules[8] = "\)" at position 7 with len 1: )
[src/monitor/debug/expr.c,91,make_token] match rules[4] = "\-" at position 8 with len 1: -
[src/monitor/debug/expr.c,91,make_token] match rules[10] = "[0-9]+" at position 9 with len 2: 20
[src/monitor/debug/expr.c,91,make_token] match rules[1] = "\+" at position 11 with len 1: +
[src/monitor/debug/expr.c,91,make_token] match rules[7] = "\(" at position 12 with len 1: (
[src/monitor/debug/expr.c,91,make_token] match rules[11] = "\$(\$0|ra|[sgt]p|t[0-6]|a[0-7]|s([0-9]|1[0-1]))"
[src/monitor/debug/expr.c,91,make_token] match rules[5] = "\*" at position 16 with len 1: *
[src/monitor/debug/expr.c,91,make_token] match rules[10] = "[0-9]+" at position 17 with len 2: 10
[src/monitor/debug/expr.c,91,make_token] match rules[8] = "\)" at position 19 with len 1: )
[src/monitor/debug/expr.c,91,make_token] match rules[5] = "\*" at position 20 with len 1: *
[src/monitor/debug/expr.c,91,make_token] match rules[7] = "\(" at position 21 with len 1: (
[src/monitor/debug/expr.c,91,make_token] match rules[11] = "\$(\$0|ra|[sgt]p|t[0-6]|a[0-7]|s([0-9]|1[0-1]))"
[src/monitor/debug/expr.c,91,make_token] match rules[5] = "\*" at position 25 with len 1: *
[src/monitor/debug/expr.c,91,make_token] match rules[10] = "[0-9]+" at position 26 with len 1: 5
[src/monitor/debug/expr.c,91,make_token] match rules[8] = "\)" at position 27 with len 1: )
[src/monitor/debug/expr.c,91,make_token] match rules[8] = "\)" at position 28 with len 1: )
 ((10*10)-20+($tp*10)*($s0*5)) = 80(0x50) ;
```

5. 监视点相关

```
(nemu) w $s0=10
$s0=10[src/monitor/debug/expr.c,91,make_token] match rules[11] = "\$(\$0|ra|[sgt]p|t[0-6]|a[0-7]|
s0
no match at position 3
$s0=10
   ^
NO.0 watchpoint is setted.
(nemu) w $t0*5
$t0*5[src/monitor/debug/expr.c,91,make_token] match rules[11] = "\$(\$0|ra|[sgt]p|t[0-6]|a[0-7]|s
0
[src/monitor/debug/expr.c,91,make_token] match rules[5] = "\*" at position 3 with len 1: *
[src/monitor/debug/expr.c,91,make_token] match rules[10] = "[0-9]+" at position 4 with len 1: 5
NO.1 watchpoint is setted.
(nemu) info w
NUM                 VALUE                  EXPR
1               0(0x0       )               $t0*5
0               0(0x0       )               $s0=10
(nemu) d 1
[src/monitor/debug/expr.c,91,make_token] match rules[10] = "[0-9]+" at position 0 with len 1: 1
(nemu) info w
NUM                 VALUE                  EXPR
0               0(0x0       )               $s0=10
(nemu)
```

所有功能均实现完毕

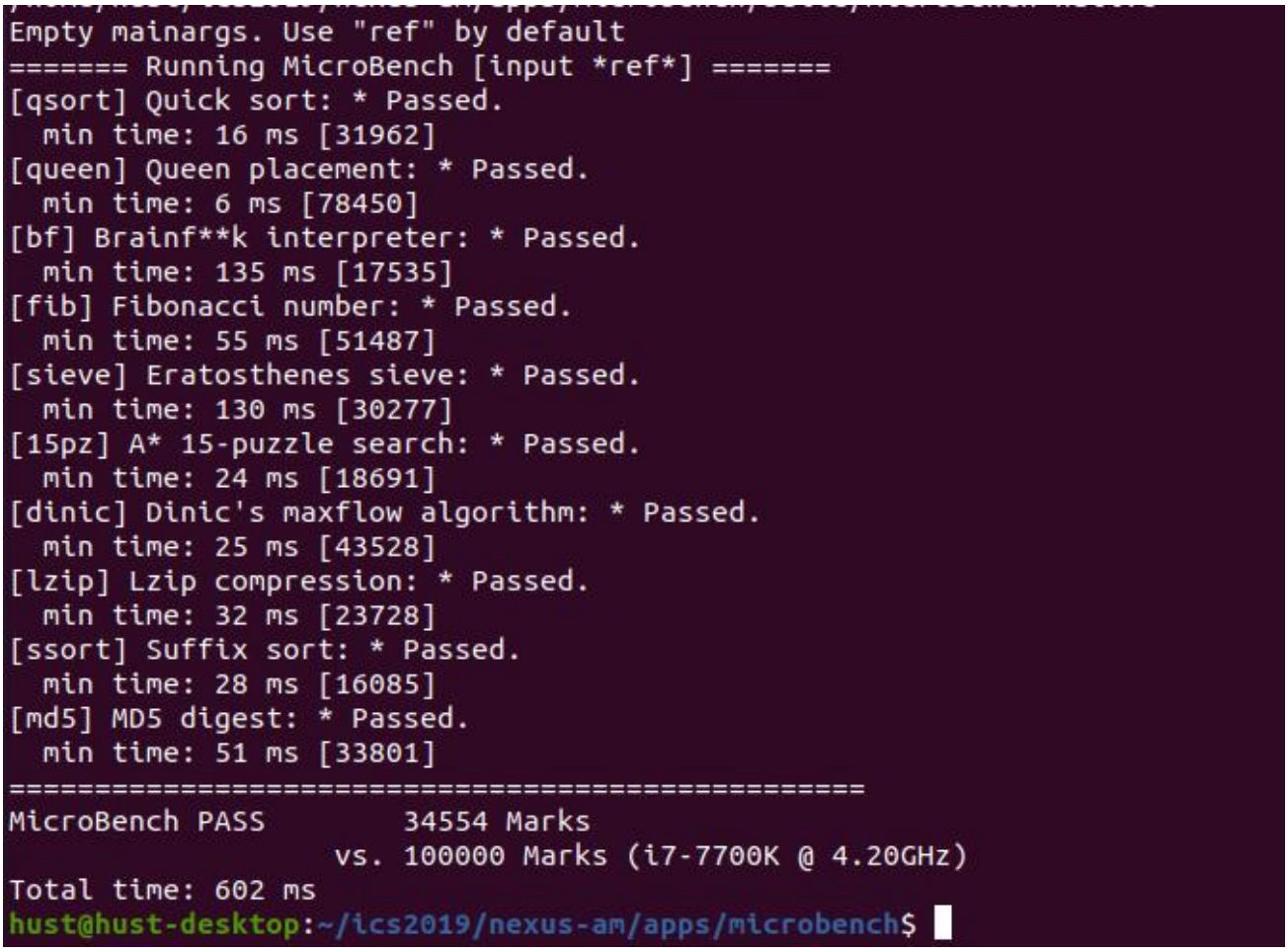
PA2

> 以下测试一部分是在macbook中的virtualbox虚拟机中运行的，一部分是在一台双系统的ubuntu中运行的

1. runall.sh回归测试脚本

```
[   add-longlong] PASS!
[            add] PASS!
[            bit] PASS!
[    bubble-sort] PASS!
[            div] PASS!
[          dummy] PASS!
[           fact] PASS!
[            fib] PASS!
[       goldbach] PASS!
[      hello-str] PASS!
[        if-else] PASS!
[      leap-year] PASS!
[     load-store] PASS!
[     matrix-mul] PASS!
[            max] PASS!
[           min3] PASS!
[          mov-c] PASS!
[          movsx] PASS!
[   mul-longlong] PASS!
[         pascal] PASS!
[          prime] PASS!
[     quick-sort] PASS!
[      recursion] PASS!
[    select-sort] PASS!
[          shift] PASS!
[    shuixianhua] PASS!
[         string] PASS!
[   sub-longlong] PASS!
[            sum] PASS!
[         switch] PASS!
[ to-lower-case] PASS!
[        unalign] PASS!
[         wanshu] PASS!
```

2. Microbench



3. ppt演示

基于AM的教学生态系统

- 第一届龙芯杯比赛，南京大学一队展示在CPU上运行教学操作系统Nanos和仙剑奇侠传

(a) Linux native, back-ended with SDL2 (screenshot)

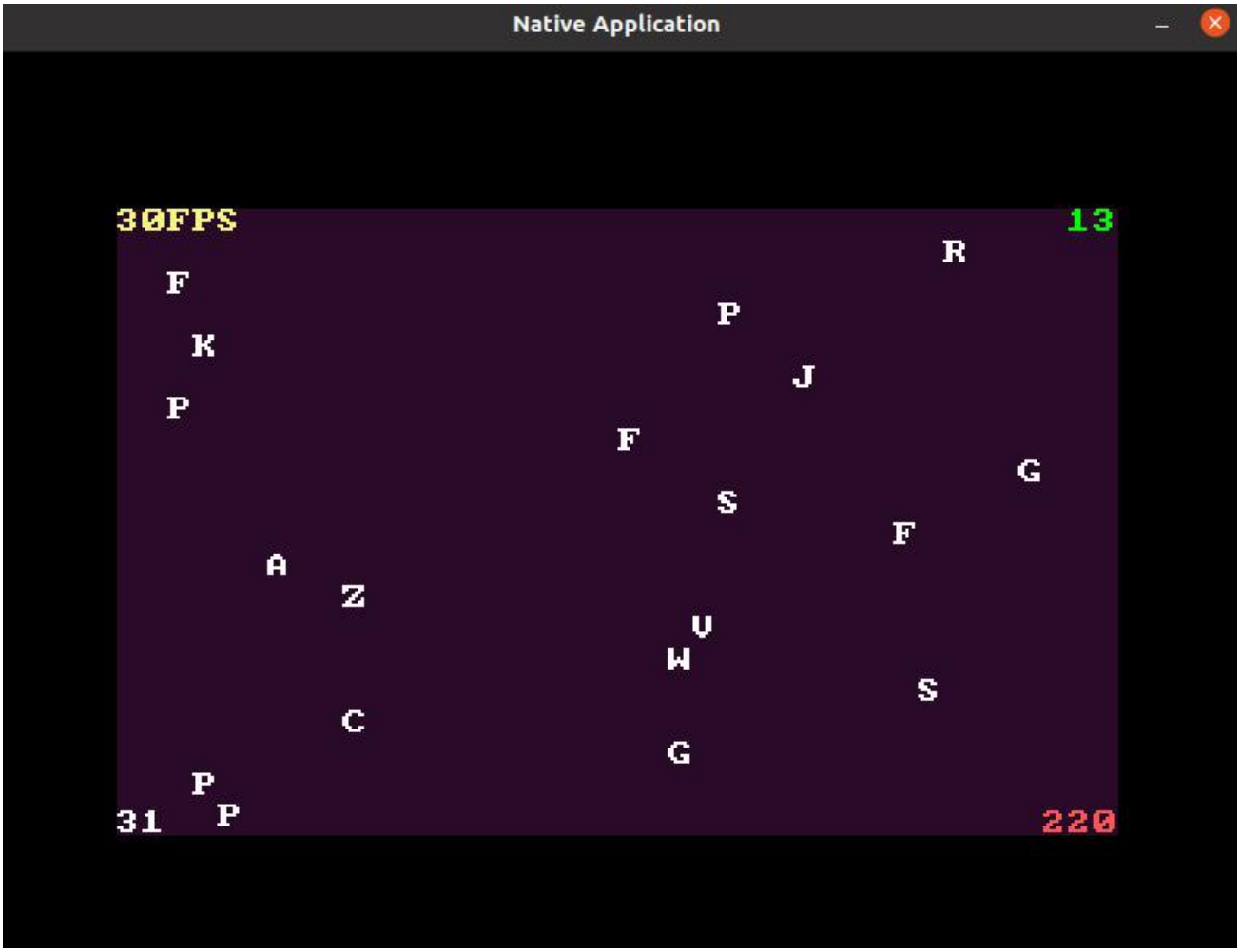
(b) a teaching x86 full system emulator (screenshot)

(c) a teaching MIPS32 SoC (FPGA, only TRM and IOE)

(d) a teaching OS (with GUI) and MIPS32 SoC (FPGA)

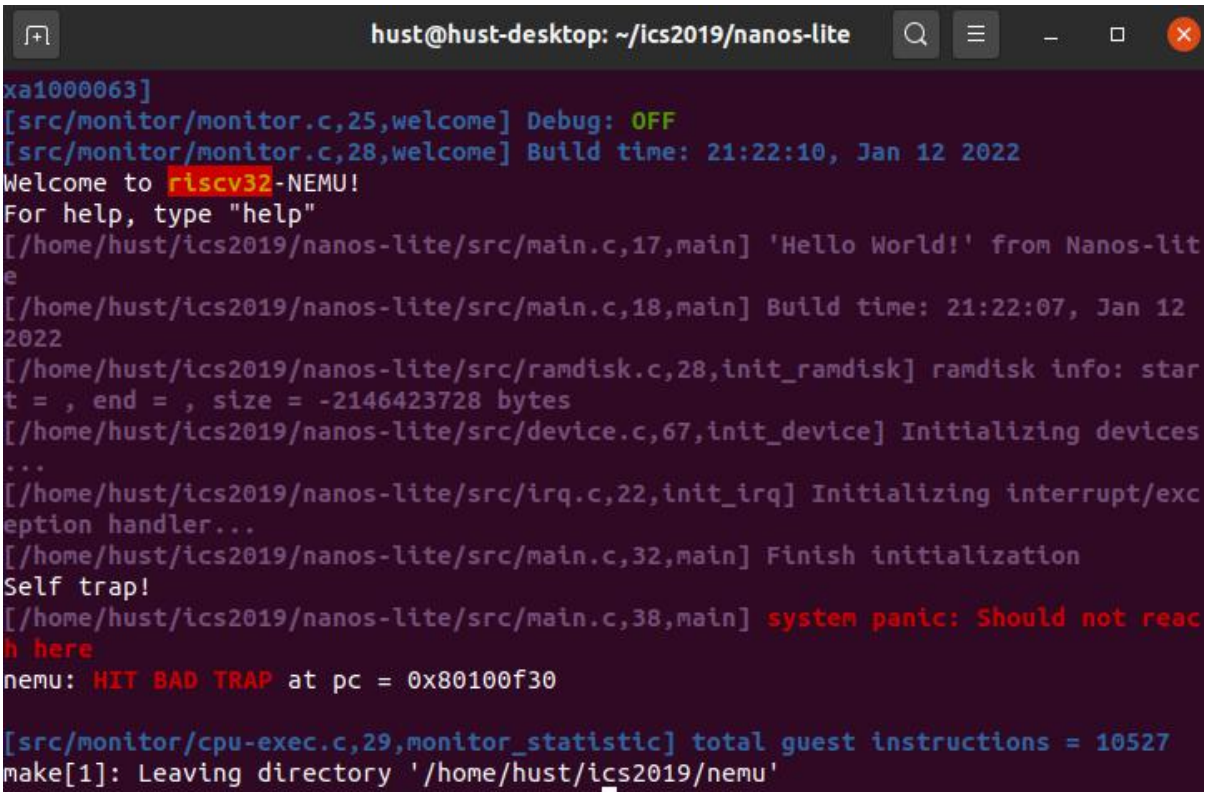
Figure 4. The same LiteNES emulator running on different platforms.

4. 打字游戏



PA3

3.1 异常自陷操作



三、心得建议

这次的项目花费了蛮长的时间去进行，中间涉及到了很多知识，中途也遇到了许多困难，但是都坚持了下来，最后终于完成了PA1，PA2以及PA3的大部分内容。

PA1实现表达式和监视点需要书写较多的代码，别的大部分都是基础功能，是整个PA项目的开始，也是整个PA项目的基础，所以这些文件都位于debug目录下，其实也是在暗示我们PA1实现得好有助于后面的调试，虽然说后面其实并没有使用PA1实现的简易调试器，但还是很有参考价值的。

PA2实现指令集，由于指令比较多，而且汇编的知识也基本忘记了，所以花费了许多时间才完成，中间也遇到了非常非常多的bug，不过后来也慢慢地发现了各个指令之间的共通之处，降低了实现的难度，最终也总算完成跑分以及PPT和打字游戏。

PA3实现了异常的自陷操作，也对nanos-lite中src的各个文件进行了内容实现，也实现了系统调用，大部分的功能都已经实现，但由于程序仍然存在bug，所以并没有成功运转仙剑奇侠传，也是一个遗憾吧。

希望以后还能够有机会进行类似的实验，不断地进行自我提高。